

**IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA
CHARLESTON**

IN THE MATTER OF THE SEARCH OF:

**Content of files submitted CASE NO. 2:23-mj-00131
In connection with CyberTipline
Report #152629859, currently in
the custody of Homeland
Security Investigations, and
more fully described in
Attachment A.**

AFFIDAVIT

Your Affiant, Christopher Yarnell, having been duly sworn, does hereby depose and state that the following is true to the best of my information, knowledge, and belief:

I. INTRODUCTION

1. I am a Special Agent with Homeland Security Investigations ("HSI"). I have been so employed since June 2017. Prior to my employment with HSI, I was a Border Patrol Agent and a Task Force Officer with HSI. I am a graduate of three federal law enforcement academies at the Federal Law Enforcement Training Centers ("FLETC"). I graduated from the United States Border Patrol Agent Academy in 2008, Criminal Investigator Training Program in 2017, and the HSI Special Agent Training Program in 2018. As part of some of these programs, I received extensive training in the areas of law within the jurisdiction of HSI. I have specifically received

training in the areas of child pornography and the sexual exploitation and abuse of children. This training included specialized instruction on how to conduct criminal investigations related to violations of child protection laws pursuant to 18 U.S.C. §§ 2251, 2252, 2252A, and 2256.

2. I am currently assigned to the HSI Resident Agent in Charge, Charleston, West Virginia. During my tenure with HSI, I have participated in, and gained experience with, conducting investigations involving computers and the processes that are necessary to retrieve, collect, and preserve electronic evidence. Through my training and experience, including work-related discussions with other law enforcement agents, I am familiar with the operational techniques and organizational structure of child pornography distribution networks, as well as the traits and characteristics of child pornography collectors and possessors and their use of computers or other electronic and media devices to facilitate the collection, possession, trade, distribution, access, and receipt of child pornographic materials. I have received training in the areas of child pornography and child exploitation and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in the form of computer media. Moreover, I am a federal law enforcement

officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, 2252A, and 2256.

6. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property-file(s) submitted in connection with Cyber Tipline Report #152629859 ("the CyberTip"), which are currently in the possession of law enforcement. The files submitted in connection with the CyberTip (more fully described in Attachment A), and the data located therein, there being probable cause to believe that located in the place described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer, and 18 U.S.C. § 2252A(a)(1), transportation of child pornography in interstate commerce.

7. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1), transportation of child pornography in

interstate commerce; 2252A(a)(2), receiving and distributing child pornography in interstate commerce by computer; and § 2252A(a)(5)(B), possession of child pornography; and are located in the place described in Attachment A.

8. The information contained within the Affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

II. RELEVANT STATUTES

9. The investigation concerns potential violations of 18 U.S.C. §§ 2252A(a)(1), (2), and (5)(B), relating to matters involving the sexual exploitation of minors.

- a. 18 U.S.C. 2252A(a)(1) prohibits any person from knowingly mailing, transporting, or shipping child pornography in interstate or foreign commerce by any means, including by computer.
- b. 18 U.S.C. § 2252A(a)(2) prohibits any person from knowingly receiving or distributing any child pornography that has been mailed or shipped or transported in interstate or foreign commerce by any means, including by computer.
- c. 18 U.S.C. § 2252A(a)(5)(B) prohibits any person from knowingly possessing any books, magazines, periodicals films, video tapes, computer discs, or

other matter that contains an image of child pornography that has been mailed, shipped, or transported in interstate or foreign commerce by any means, including computer, or that was produced using materials mailed, shipped, or transported in interstate or foreign commerce by any means, including computer.

III. DEFINITIONS

10. The following terms are relevant to this Affidavit in support of this application for a search warrant:

- a. Child Erotica: The term "child erotica" means any material relating to minors that serves a sexual purpose for a given individual, including fantasy writings, letters, diaries, books, sexual aids, souvenirs, toys, costumes, drawings, and images or videos of minors that are not sexually explicit.
- b. Child Pornography: The term "child pornography" is defined at 18 U.S.C. § 2256(8). It consists of a visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a

minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct), as well as any visual depiction, the production of which involves the use of a minor engaged in sexually explicit conduct. See 18 U.S.C. §§ 2252 and 2256(2), (8).

- c. Internet Protocol ("IP") Address: An "IP address" is a unique number used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom

IP addresses are assigned on particular dates and times.

- d. Minor: The term "minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
- e. Sexually Explicit Conduct: The term "sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).
- f. Visual Depictions: "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

IV. CYBERTIPLINE REPORT AND PROBABLE CAUSE

11. The National Center for Missing and Exploited Children ("NCMEC") is an organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography.

12. Companies that suspect child pornography has been stored or transmitted on their systems can report that

information to NCMEC in a CyberTip. To make such a report, a company providing services on the internet, known as an electronic service provider ("ESP"), can go to an online portal that NCMEC has set up for the submission of these tips. The ESP, in this case Snapchat, can then provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen or usernames associated with the activity, any IP address or port numbers it captured, chat history records, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and incident time, the remainder of the information the ESP provides is voluntary and undertaken at the initiative of the reporting ESP. The ESP may also upload to NCMEC any files it collected in connection with the activity. The ESP may or may not independently view the content of the files it uploads.

13. NCMEC does not review the content of these uploaded files not previously viewed by the ESP. Using publicly available search tools, NCMEC attempts to locate where the activity occurred based on the information the ESP provides, such as IP addresses. NCMEC packages the information from the ESP along with any additional information it has, such as previous related CyberTips, and sends it to law enforcement

in the jurisdiction where the activity is thought to have occurred.

14. On or about January 14, 2023, electronic service provider Snapchat submitted Cyber Tipline Report #152629859 to NCMEC. The incident type was identified as apparent child pornography, and the incident time was listed as: January 13, 2023, at 12:17:22 UTC. NCMEC classifies the Cybertip as Apparent Child Pornography Files Not reviewed by NCMEC, Hash Match.

15. Snapchat provided two files in connection with the report. The first file bears filename abibeav-None-cbf4d145-72a3-5b78-8c34-c9d3c3c3efce~39-6dd8541531.mp4, and the content of which was not reviewed by NCMEC or Snapchat. The second file, bearing filename abibeav-None-cbf4d145-72a3-5b78-8c34-c9d3c3c3efce~29-66a903c7c2.mp4, was not reviewed by NCMEC; however, Snapchat viewed the file. The second file contained an alleged media file of apparent child pornography. Specifically, the file contained an approximate twenty-four (24) second video of a nude, toddler-aged female child being forced to perform fellatio on an adult male's erect penis.

16. NCMEC used publicly available search tools to discover that the IP address the ESP reported resolved to Suddenlink Communications in the Charleston, WV area. The

CyberTip was then provided to law enforcement in this jurisdiction.

17. I know from my training and experience that hash values are widely used by most ESPs and others, including law enforcement, to identify files. A hash value is akin to a fingerprint for a file. A hash value is obtained by processing the contents of a file through a cryptographic algorithm, which produces a unique numerical value, the hash value, which identifies the unique contents of the file. If the contents of the file are modified in any way, the value of the hash will also change.

18. I know from my training and experience that many ESPs compare the hash values of files that its customers transmit on its systems against a database containing hash values of known child pornography material. If the ESP finds that a hash value on its system matches one in the database, the ESP captures the file along with information about the user who uploaded, posted, possessed, or otherwise transmitted the file on the ESP's systems. This information is then transmitted to NCMEC in the form of a Cybertip.

19. The image file at issue here, abibeav-None-cbf4d145-72a3-5b78-8c34-c9d3c3c3efce~39-6dd8541531.mp4, was flagged by the ESP based on a hash match.

20. Based on information contained in the Cybertip, it indicates that Snapchat did not review file abibeav-None-cbf4d145-72a3-5b78-8c34-c9d3c3c3efce~39-6dd8541531.mp4 submitted in connection with the Cybertip. Although Snapchat did not review this material, I have probable cause to believe the material contains relevant information related to the possession of child pornography, by virtue of Snapchat including it in the Cybertip reporting child pornography.

21. In or about February 2023, another agent at HSI was working on this investigation and viewed the file attached to the Cybertip outlined above. Once the agent determined that this file had not been viewed by Snapchat, he immediately flagged the issue. Your Affiant then took over the investigation and now makes application for this search warrant.

22. In summary, there is probable cause to believe that the material in the file abibeav-None-cbf4d145-72a3-5b78-8c34-c9d3c3c3efce~39-6dd8541531.mp4 that Snapchat sent to NCMEC in connection with the Cybertip contains relevant data related to the sexual exploitation of children, including any material that may not have been previously reviewed by Snapchat.

V. INTERSTATE NEXUS

23. I submit that the element of "in or affecting interstate or foreign commerce" is satisfied for a violation of 18 U.S.C. § 2252A, for the limited purpose of securing a search warrant, through use of the ESP servers and use of the Internet in connection with this offense.

VI. CONCLUSION

24. Based on the aforementioned factual information, your Affiant respectfully submits that there is probable cause to believe that inside the files that Snapchat provided in connection with the above Cybertip #152629859 (described in Attachment A), will be found evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A(a)(1), transportation of child pornography; 2252A(a)(2), receiving and distributing child pornography in interstate commerce; and 18 U.S.C. § 2252A(a)(5)(B), possession of child pornography (described in Attachment B) will be found.

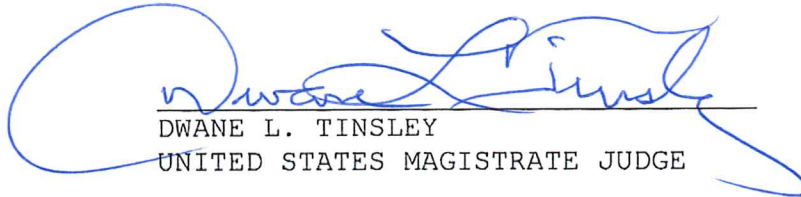
25. Your Affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search and seizure of the items described in Attachment A, for the items listed in Attachment B.

I swear that this information is true and correct to the best of my knowledge.



SPECIAL AGENT CHRISTOPHER A. YARNELL
DEPARTMENT OF HOMELAND SECURITY
HOMELAND SECURITY INVESTIGATIONS

SUBSCRIBED and SWORN to before me by telephonic means
this 18th day of July, 2023.



DWANE L. TINSLEY
UNITED STATES MAGISTRATE JUDGE